Quantum Information and Computation, Vol. 1, No. 0 (2001) 000–000

QUANTUM VERNAM CIPHER

DEBBIE W. LEUNG
IBM T.J. Watson Research Center, P.O. Box 218
Yorktown Heights, New York 10598, USA

May 7, 2001

We discuss aspects of secure quantum communication by proposing and analyzing a quantum analog of the Vernam cipher (one-time-pad). The quantum Vernam cipher uses entanglement as the key to encrypt quantum information sent through an insecure quantum channel. First, in sharp contrast with the classical Vernam cipher, the quantum key can be recycled securely. We show that key recycling is intrinsic to the quantum cipher-text, rather than using entanglement as the key. Second, the scheme detects and corrects for arbitrary transmission errors, and it does so using only local operations and classical communication (LOCC) between the sender and the receiver. The application to quantum message authentication is discussed. Quantum secret sharing schemes with similar properties are characterized. We also discuss two general issues, the relation between secret communication and secret sharing, the classification of secure communication protocols.

Keywords: Private key encryption, key recycling, secret sharing, authentication

1. Introduction

Recent developments in quantum information theory have brought many surprises in cryptology. A partial list includes an efficient quantum algorithm for factoring [1] which can break the condition for security in many cryptographic protocols, unconditionally secure quantum key distribution protocols [2,3,4,5], and a no-go theorem for unconditionally secure quantum bit commitment [6,7]. Cryptographic protocols for quantum information are also being developed. For examples, see Refs. 8, 9, 10, 11, 12, 13.

Emerging from these interesting results are important open questions on what quantum mechanics admits and prohibits in cryptography and the reasons why. This paper reports partial progress along this direction, by analyzing a proposed "quantum Vernam cipher" which encrypts a quantum plain-text to a quantum cipher-text using *entanglement* as a "key". The proposed scheme is a quantum analog of various existing schemes, including the classical Vernam cipher [14] (one-time-pad) in which all of the plain-text, the cipher-text, and the key are classical, the eavesdrop-detecting channel [15], in which the plain-text and the key are classical but the cipher-text is quantum, and the private quantum channel [8,9] in which the plain-text and the cipher-text are quantum but the key is classical.

One intriguing property of the quantum Vernam cipher is that the key can be recycled

securely using test and purification procedures for entanglement [5,16].[a] As a comparison, key recycling is insecure in the classical Vernam cipher [19] but secure in the eavesdrop-detecting channel [15]. These observations suggest that the security of key recycling comes from the possibility to detect eavesdropping in the quantum cipher-text, rather than using entanglement as a key. We give further support to this suggestion by modifying the private quantum channel to securely recycle the classical key.

Another intriguing property of the quantum Vernam cipher is the ability to correct for *any* damage on the transmitted quantum state. Moreover, the correction procedure involves only classical communication between the sender and the receiver. These can be explained by the theory of quantum secret sharing [10,11]. Quantum secret sharing schemes with similar properties are characterized. We discuss general connections between secret communication and secret sharing, and apply the connections to other secret communication schemes.

As suggested by the above results, and in concert with our effort to relate cryptographic properties to various elements in cryptographic schemes, we classify existing schemes according to the classical or quantum nature of the communication channel and the key (the resources) and the plain-text (the application), and consider the security of key recycling and reliability for each class. Besides the schemes mentioned above, teleportation [20], superdense coding [21], and key distribution protocols [2,3] are also included.

Secure key recycling and reliability are closely related to message authentication. We briefly discuss applications of our analysis to the authentication of quantum messages [12,13].

Despite the fact that entanglement is recycled in the quantum Vernam cipher, we find that, given the same resources, secure quantum communication can be more efficiently realized by distributing entanglement and then teleporting the state. We emphasize that our main goal is to understand and analyze security in quantum protocols; our proposed cipher and the comparisons with other schemes are tools for doing so.

This paper is structured as follows. The quantum Vernam cipher is described in Section 2 following the reviews of private key encryption and the private quantum channel. Eavesdropping and error correction strategies are explained in Section 3. Key recycling is analyzed in Section 4. The connections between secret communication and secret sharing are discussed in Section 5. We conclude with a classification of secure communication protocols, some applications of the analysis to authentication, and some open questions. For completeness, various relevant cryptographic schemes are described in Appendices A, C, and D.

1.1. *Definitions and Assumptions*

In communication problems, the sender, the receiver, and any adversary (such as an eavesdropper) are traditionally called Alice, Bob, and Eve respectively. For simplicity in

[a] A recent article [17] has *independently* reported using entanglement as a recyclable quantum key to conceal classical information. The application to encrypt quantum information was suggested but not accomplished [18].

notation and in the proofs, we make the following assumptions throughout the paper.

- Channel noise and logical errors are negligible.
- Alice and Bob have a 2-way classical *broadcast* channel. Hence classical communication is public but unjammable and authenticated (not forged or tampered with).
- Alice and Bob may also be given a quantum channel or entanglement. Such quantum channel is assumed insecure, while the given entanglement is pure and authenticated.

The two quantum resources are inequivalent. Entanglement can be converted to a secure quantum channel by teleportation (see Appendix A). A quantum channel which is insecure can establish "mixed entanglement", but further test and distillation procedures [16,5] are needed to establish pure entanglement.

2. Concealing Ciphers

In this section, we describe the quantum Vernam cipher. We first review basic notions in private key encryption, using the classical Vernam cipher, the eavesdrop-detecting channel, and the private quantum channel as examples. These examples also motivate the construction of the quantum Vernam cipher. We concentrate on the ability to conceal the communicated secret from an eavesdropping adversary. Other aspects of security will be discussed later.

2.1. *Private key encryption*

In secret classical communication using private key encryption, Alice and Bob share a secret string K, called the "key", which encrypts (locks) a message M from Eve during transmission and decrypts (opens) M for Bob afterwards.

For example, in the Vernam cipher [14], a *random* n-bit key K is used to encrypt an n-bit message M (also known as the *plain-text*). Alice sends a *cipher-text* $C = M \oplus K$ to Bob, where $\oplus$ denotes bitwise XOR (addition modulo 2). Bob decodes by calculating $C \oplus K = M$. Shannon proved that [19] the Vernam cipher is *absolutely secure*:[b] C is random and *independent* of M when K is random and unknown. Shannon also proved that absolute security requires the entropy (thus the length) of K to be at least n. Thus reusing a key, even with privacy amplification [22], compromises security when previously transmitted cipher-text might have been tapped.

As another example, we consider a simple case of the eavesdrop-detecting channel [15]. Let r be a security parameter. An n-bit classical plain-text M is encrypted with two $(n+r)$-bit classical keys K_1, K_2 into a *quantum* cipher-text as follows. Alice concatenates M with r random subset parities of M to form M'. She sends each bit of $K_1 \oplus M'$ in the basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ depending on each bit of K_2. After Bob receives and decodes the cipher-text, Alice announces the random subsets. The decoded message is accepted only if all the subset parities are correct. In this case, the keys can be reused

[b] A cipher is absolutely secure if C and M are independent.

(with privacy amplification), because, when l bits of the cipher-text have been intercepted, the probability to have no inconsistencies in the subset parities is no more than $(\frac{3}{4})^{-l}$.

2.2. *Private quantum channel*

We motivate the quantum Vernam cipher by reviewing the following canonical example of the private quantum channel [8,9], which uses a classical key to encrypt a quantum plain-text to a quantum cipher text. For simplicity, we call the canonical example the private quantum channel. Let

$$\begin{aligned} I &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \\ X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad ZX = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \end{aligned} \tag{1}$$

denote the 2×2 identity and three "Pauli matrices". To send one quantum bit (qubit) given by the density matrix ρ, Alice and Bob share a 2-bit key $K = (k_1, k_2)$. Alice applies $Z^{k_2} X^{k_1}$ to ρ and sends to Bob the resulting "cipher-text" $\rho' = Z^{k_2} X^{k_1} \rho X^{k_1} Z^{k_2}$, which is decoded by Bob by applying $X^{k_1} Z^{k_2}$. From Eve's point of view, Alice is sending ρ, $X\rho X$, $Z\rho Z$, and $ZX\rho XZ$ at random; she sees a mixture $\frac{I}{2}$ which is independent of ρ. To send an n-qubit state ρ, the 1-qubit scheme is applied bitwise. Let K be a $2n$-bit classical key with i-th bit k_i. Let X_i and Z_i denote X and Z acting on the i-th qubit. Alice sends to Bob $\rho' = U_K \rho U_K^\dagger$, where $U_K = \bigotimes_i Z_i^{k_{2i}} X_i^{k_{2i-1}}$. Bob applies $U_K^\dagger$ to recover ρ from ρ'. Eve sees a mixture of uniformly distributed possible states:

$$\frac{1}{2^{2n}} \sum_K U_K \rho U_K^\dagger = \frac{1}{2^n} I^{\otimes n}, \tag{2}$$

which is independent of ρ.[c] It was also proved in Ref. 8 that $H(K) \geq 2n$ is necessary to completely randomize an arbitrary ρ. A schematic diagram is given in Fig. 1.

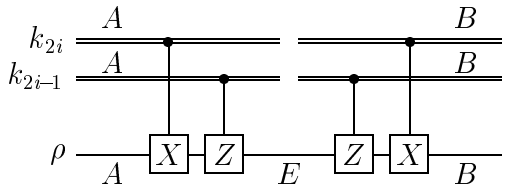


Fig. 1. The private quantum channel. Time runs from left to right. A, B, and E stand for Alice, Bob, and Eve and denote the owners of the registers. Double lines represent classical bits. X and Z are applied to the quantum state if their respective classical control bits equal 1. These conventions are assumed throughout the paper.

[c] Equation (2) can be derived using the Pauli decomposition of ρ: each nontrivial component anticommutes with half of the U_K and vanishes in the sum, leaving only the identity term.

2.3. *The quantum Vernam cipher*

We use entanglement as the key in our quantum Vernam cipher. The fundamental unit of entanglement is an "ebit". Alice and Bob are said to share an ebit if each possesses one qubit of a *known* maximally entangled state of two qubits, such as the EPR states $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$. The procedure to transmit one qubit using two ebits is summarized in Fig. 2.

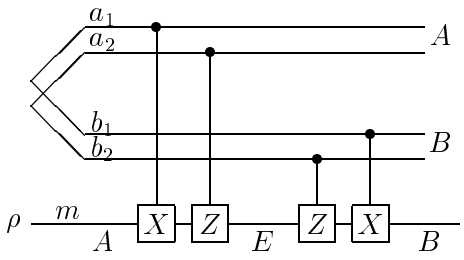


Fig. 2. The quantum Vernam cipher to send one qubit.

The registers in Fig. 2 are labeled by a_1, a_2, b_1, b_2, and m. $\{a_1, b_1\}$ and $\{a_2, b_2\}$ are initially in the state $|\Phi^+\rangle$. The registers a_1, a_2 belong to Alice and b_1, b_2 belong to Bob all the time. The register m initially carries the message ρ and belongs to Alice. Alice applies a controlled-X (CNOT) from a_1 to m and a controlled-Z (CZ) from a_2 to m and sends m to Bob. We assume Eve takes control of m during the transmission. When Bob receives m, he applies a CZ from b_2 to m, followed by a CNOT from b_1 to m to recover ρ. To send an n-qubit state ρ, the one-qubit protocol is applied bitwise. We show that the quantum Vernam cipher is a *purification* of the private quantum channel, superposing all possible key states: The key registers $(a_1, b_1, \cdots, a_{2n}, b_{2n})$ have initial state $|\Phi^+\rangle^{\otimes 2n}$. Reordering the qubits as $(a_1, \cdots, a_{2n}, b_1, \cdots, b_{2n})$, the initial key state $\frac{1}{2^n}\sum_K |K\rangle|K\rangle$, where K ranges over all $2n$-bit strings, is indeed the superposition of all possible classical keys. Finally, the quantum Vernam cipher and the private quantum channel have *equivalent* encoding and decoding operations, establishing the claim. Eve sees a cipher-text described by tracing out the subsystem $\{a_1, \cdots, a_{2n}, b_1, \cdots, b_{2n}\}$, which corresponds to averaging over all possible keys $|K\rangle|K\rangle$. Following the discussion in Section 2.2, Eve sees the state $I^{\otimes n}/2^n$. Thus Eve obtains no information on ρ.

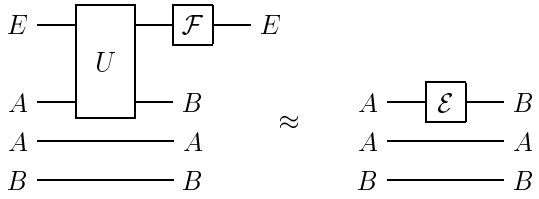
In the absence of eavesdropping, the circuit in Fig. 2 acts trivially, so that ρ is recovered, and the key $|\Phi^+\rangle^{\otimes 2n}$ is regenerated. We now consider the effects of eavesdropping.

3. Eavesdropping and Error Correction

Even though Eve obtains no information from the cipher-text, she may disturb, destroy, or alter it, and entangle her ancilla with the quantum key to be regenerated. In this section, we describe the effects of eavesdropping and a basic correction method, which are starting points for our discussions in Sections 4 and 5.

3.1. *General eavesdropping and correction strategy*

We assume that the plain-text is initially disentangled from Eve. Eve's most general strategy is to apply a joint unitary operation U on the transmitted cipher-text and a pure state ancilla of hers, and send Bob "something". We may assume she outputs the correct number of qubits as Bob can add or discard qubits. Note that there is no further communication from Eve to Alice or Bob. Thus subsequent action $\mathcal{F}$ by Eve on her ancilla *cannot* change the superoperator $\mathcal{E}$ that describes the transmission of the cipher-text. The situation is summarized as



A convenient representation of $\mathcal{E}$ is given by [23,24]

$$\mathcal{E}(\rho) = \sum_{ij} e_{ij} P_i \rho P_j^\dagger \tag{3}$$

where e_{ij} are entries of a positive matrix and the sum is over all Pauli matrices P_i on the n-qubit cipher-text. Equation (3) can be interpreted as a process that transforms a state ρ into a mixture $\sum_k D_k \rho D_k^\dagger$ where D_k are noninterfering errors. Expressing each D_k as a linear combination of Pauli matrices, one obtains Eq. (3). The P_i in Eq. (3) thus represent errors that may interfere with each other. Using the language of quantum error correction, we call the P_i Pauli errors. We now show that if Alice and Bob determine with high probability what Pauli error has occurred, their final state is almost disentangled from Eve. The process of determining the error is called *syndrome extraction*.

The cipher-text is generally *part of* a state $\tilde{\rho}$ obtained from encoding the plain-text with some ancilla. The state possessed by Alice and Bob after the transmission is given by

$$(\mathcal{I} \otimes \mathcal{E})(\tilde{\rho}) = \sum_{ij} e_{ij} (I \otimes P_i) \tilde{\rho} (I \otimes P_j^\dagger) \tag{4}$$

where the identity operator $\mathcal{I}$ acts on the uncommunicated subsystem.

First suppose it is possible to *perfectly* distinguish the states $(I \otimes P_i)\tilde{\rho}(I \otimes P_i^\dagger)$ nondestructively. Then, there is a projective measurement $\mathcal{Q}$ with projectors Q_i such that

$$\text{if } j = i \quad Q_i (I \otimes P_j) \tilde{\rho} (I \otimes P_j^\dagger) Q_i = (I \otimes P_j) \tilde{\rho} (I \otimes P_j^\dagger) \tag{5}$$

$$\text{if } j \neq i \quad Q_i (I \otimes P_j) \tilde{\rho} (I \otimes P_j^\dagger) Q_i = 0 \tag{6}$$

Since $\tilde{\rho}$ is positive, Eqs. (5) and (6) are equivalent to

$$\text{if } j = i \quad Q_i (I \otimes P_j) \tilde{\rho} = (I \otimes P_j) \tilde{\rho} \tag{7}$$

$$\text{if } j \neq i \quad Q_i (I \otimes P_j) \tilde{\rho} = 0 \tag{8}$$

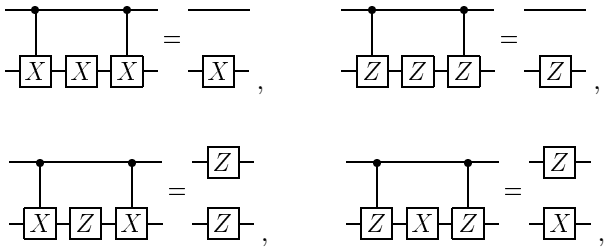
The projector Q_i *removes* any term in Eq. (4) with a P_j for all $j \neq i$, leaving only the output $(I \otimes P_i)\tilde{\rho}(I \otimes P_i^\dagger)$, which is independent of $\mathcal{E}$ and disentangled from Eve.

We consider situations deviating from the above perfect scenario. For example, the measurement outcome i may be accompanied by some irreversible state change O_i. Moreover, the measurement may only distinguish subsets of errors or be probabilistic, so that multiple terms in Eq. (4) may remain in the final state. However, if a syndrome i is extracted with high probability, the post-measurement state has density matrix dominated by $O_i(I \otimes P_i)\tilde{\rho}(I \otimes P_i^\dagger)O_i^\dagger$, and is almost disentangled from Eve.

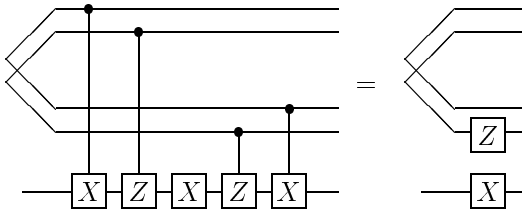
Suppose Alice and Bob reuse a private key obtained from $(\mathcal{I} \otimes \mathcal{E})(\tilde{\rho})$ which is entangled with Eve. Eve can learn about the future communication or correlate different rounds of communicated materials only through the correlation with the reused private key. Such correlation is small when syndrome extraction succeeds with high probability, in which case Eve has little information on any nontrivial function on all the plain-text. Key recycling is then *semantically secure* [25]. A scheme is *semantically secure* [25], if there is vanishing difference between the probabilities to estimate the value of any nontrivial function on the plain-text, with or without the cipher-text.

3.2. *Error correction for the quantum Vernam cipher*

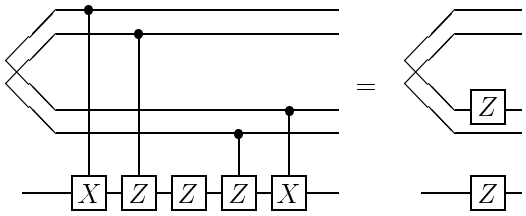
Recall that it suffices to identify the Pauli error that occurs in the cipher-text. We show how this can be done perfectly in the quantum Vernam cipher. We use the fact that Fig. 2 acts trivially, and the commutation relations



to find the effect of errors on the cipher-text for the one-qubit protocol:



and



An X error in the transmitted cipher-text propagates to the decoded message together with a Z error on b_2, changing $\{a_2, b_2\}$ from $|\Phi^+\rangle$ into $|\Phi^-\rangle$. Likewise, a Z error turns $\{a_1, b_1\}$ into $|\Phi^-\rangle$ and an XZ error turns both EPR pairs into $|\Phi^-\rangle$. Alice and Bob can distinguish $|\Phi^+\rangle$ from $|\Phi^-\rangle$ by independently measuring their halves of the EPR pair along the $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ basis and comparing their results on a broadcast channel. Since $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$ and $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle)$, the measured state is $|\Phi^+\rangle$ ($|\Phi^-\rangle$) when their results agree (disagree). Therefore, the possible Pauli errors I, X, Z, and XZ can be perfectly distinguished and corrected. The same argument applies to transmitting n qubits.

We emphasize that this detection procedure effectively turns Eve's most general action into a Pauli error. An example to recover the message without the cipher-text is given in Appendix B.

4. Key Recycling

We have seen that the EPR pairs in the quantum Vernam cipher can be measured to extract the exact error syndrome. We now show that, when many qubits are sent, it is possible to use less entanglement (per qubit) for syndrome extraction with very high probability. The remaining EPR pairs can be recycled, with semantic security. We show strong evidence that security is due to transmitting a quantum cipher-text, rather than using entanglement as the key, by modifying the private quantum channel to recycle a classical key.

4.1. *Recycling quantum key*

Recall that after sending n qubits with the quantum Vernam cipher, Alice and Bob share $2n$ EPR pairs either in $|\Phi^+\rangle$ or $|\Phi^-\rangle$, in a one-to-one correspondence with the Pauli error in the cipher-text. Syndrome extraction is equivalent to learning the identity of these EPR pairs. Asymptotically, this can be done in two steps. The first step, adapted from Ref. 5, is a preliminary test for eavesdropping by testing if the EPR pairs are $|\Phi\rangle^{\otimes 2n}$. Without indication of eavesdropping, the decoded state is accepted, and the EPR pairs are recycled. Otherwise, a second step is performed to find the identity of the EPR pairs by a random hashing method adapted from Ref. 16. This procedure applies to the most general eavesdropping strategy.

Let the identity of the $2n$ EPR pairs be represented by a $2n$-bit string $\mathbf{v}$, with 0 and 1

corresponding to $|\Phi^+\rangle$ and $|\Phi^-\rangle$.[d] We first describe a useful protocol to obtain the *parity* of a subset of bits in $\mathbf{v}$. The "bilateral XOR" (BXOR), defined as $\mathrm{CNOT}_{a_1a_2}\times\mathrm{CNOT}_{b_1b_2}$,[e] effects the transformation:

$$|\Phi^+\rangle|\Phi^+\rangle \to |\Phi^+\rangle|\Phi^+\rangle \quad , \qquad |\Phi^-\rangle|\Phi^-\rangle \to |\Phi^+\rangle|\Phi^-\rangle\,,$$
$$|\Phi^+\rangle|\Phi^-\rangle \to |\Phi^-\rangle|\Phi^-\rangle \quad , \qquad |\Phi^-\rangle|\Phi^+\rangle \to |\Phi^-\rangle|\Phi^+\rangle\,,$$

where the qubits are ordered as a_1, b_1, a_2, b_2. The control pair (a_1, b_1) becomes the parity of the two pairs. Likewise, the parity of a subset $\{s_1, s_2, s_3, \cdots\}$ can be found by applying BXOR from an extra $|\Phi^+\rangle$ to all of $\{s_1, s_2, s_3, \cdots\}$.

For the preliminary test for eavesdropping, let r be a security parameter. Alice and Bob pick r random subsets of $\mathbf{v}$ and find their parities using r extra $|\Phi^+\rangle$.[f] If $\mathbf{v} = \mathbf{0}$, all subsets have even parities. Otherwise, each random subset has equal probability to be odd or even, and the probability of obtaining only even parities is 2^{-r}.

If all r parities are even, Alice and Bob recycle the $2n$-ebit key. The probability for Alice and Bob to miss an error in the decoded message and recycle a compromised key is

$$\mathrm{Prob}(\text{pass and erroneous}) \leq \mathrm{Prob}(\text{pass}|\text{erroneous}) = \frac{1}{2^r}$$

which can be made arbitrarily small by choosing a sufficiently large r.

If some subset has odd parity, Alice and Bob determine $\mathbf{v}$ as follows. The distribution of $\mathbf{v}$ is generally unknown. However, Alice and Bob can *estimate* the Hamming weight [g] of $\mathbf{v}$ by sampling r_2 random bits of $\mathbf{v}$. How r_2 depends on the security level can be found as follows. If the Hamming weight of $\mathbf{v}$ is αn, and $\tilde{\alpha} r_2$ 1's are sampled, Chebyshev's inequality implies $\forall \delta > 0$ $\mathrm{Prob}(|\tilde{\alpha} - \alpha| \geq \delta) < \frac{1}{4\delta^2 r_2}$.[h] Hence $\forall \epsilon > 0$, choosing $r_2 > \frac{1}{4\delta^2\epsilon}$ guarantees $\mathrm{Prob}(\alpha \in (\tilde{\alpha} - \delta, \tilde{\alpha} + \delta)) \geq 1 - \epsilon$. Thus with probability larger than $1 - \epsilon$, $\mathbf{v} \in \mathcal{T}$ the typical set of a binomial distribution with bias $\tilde{\alpha}$ and with size no greater than $2^{2nH(\tilde{\alpha}+\delta)}$. Here, H denotes the binary entropy function [26] and for simplicity $\tilde{\alpha} + \delta < \frac{1}{2}$. As each random subset parity eliminates about half of the possible values of $\mathbf{v}$, $\mathbf{v}$ can be identified with $r_3 \approx 2nH(\tilde{\alpha} + \delta)$ random subset parities. Approximately $2n(1 - H(\tilde{\alpha} + \delta))$ EPR pairs can be recycled with vanishing correlation with Eve.

Note that the preliminary test uses r ebits, and the second step uses $r_2 + r_3$ ebits. Since r and r_2 are independent of n, they are negligible for asymptotically large n. In contrast, $r_3 \propto n$. This is the reason for splitting the procedure into two steps. Finally, we use classical probabilities throughout the discussion since measurements are only made in the $|\Phi^\pm\rangle$ basis [5].

[d] This representation is a *simplified* version of that in Ref. 16.
[e] The first and second subscripts denote the control and target bits.
[f] These extra $|\Phi^+\rangle$ are unnecessary but they simplify the procedure.
[g] The Hamming weight is the number of "1" in a bit-string.
[h] The test bits are identically distributed, and *negatively* correlated, so that Chebyshev's inequality applies.

4.2. *Recycling classical key*

To illustrate that secure recycling is *not* a property special to entanglement, we adapt a scheme in Ref. 15 to recycle the classical key in the private quantum channel. The main idea is to add known test qubits to detect errors effectively. Specifically, consider sending n qubits with security parameter r. Alice encodes the n qubits with a $2n$-bit classical key as in the original scheme described in Section 2.2. She appends to the data qubits $2r$ test qubits, called $x_1, \cdots, x_r, z_1, \cdots, z_r$, in the state $|0\rangle^{\otimes r}|+\rangle^{\otimes r}$. Each test bit may be flipped $|0\rangle \to |1\rangle$, $|+\rangle \to |-\rangle$ depending on a $2r$-bit classical key. In addition, she picks $2r$ random subsets $S_{x1}, \cdots, S_{xr}$, $S_{z1}, \cdots, S_{zr}$ of the n data qubits. For each i, a CNOT is applied from each qubit in S_{xi} to x_i. Likewise, a CNOT is applied from z_i to each qubit in S_{zi}. Alice also picks r random subsets $T_{x1}, \cdots, T_{xr}$ of $\{z_1, \cdots, z_r\}$ and applies a CNOT from each $z_j \in T_{xi}$ to x_i.[i] Then, she sends all $n + 2r$ qubits to Bob. After Bob announces a receipt of all the qubits, Alice announces all $3r$ subsets. Bob decodes by inverting Alice's operation. If the test qubits are in the state $|0\rangle^{\otimes n}|+\rangle^{\otimes n}$, he accepts the decoded data qubits and recycles the classical key. The main idea behind the modification is illustrated in Fig. 3.

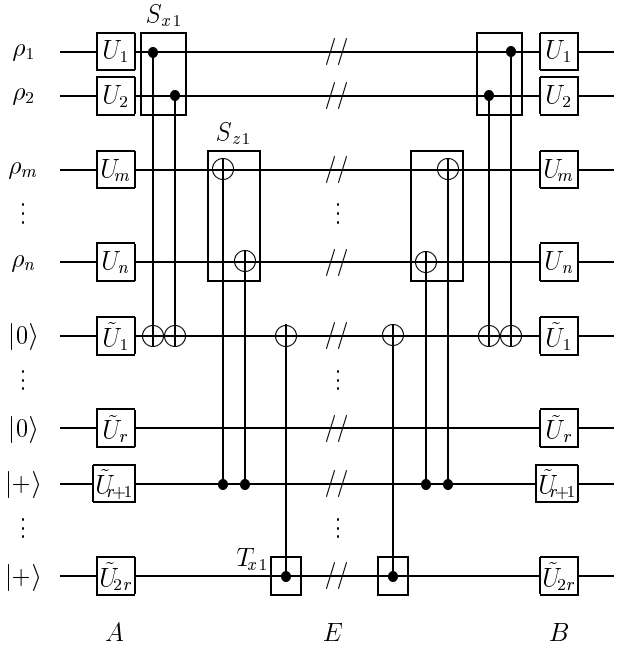


Fig. 3. The modified private quantum channel. $\rho_1, \cdots, \rho_n$ are n data qubits. Depending on the key, $U_i = I$, X, Z, or XZ, $\tilde{U}_{1,\cdots,r} = I$ or X, and $\tilde{U}_{r+1,\cdots,2r} = I$ or Z. We only show the operations related to S_{x1}, S_{z1}, and T_{x1}, with $S_{x1} = \{1, 2\}$, $S_{z1} = \{m, n\}$, and $T_{x1} = \{1\}$ as examples. The symbol // denotes a qubit in transit (and at risk).

[i] Note that $T_{x1}, \cdots, T_{xr}$ also define r random subsets $T_{z1}, \cdots, T_{zr}$ of $x_1, \cdots, x_r$ such that a CNOT is applied from z_j to each $x_i \in T_{zi}$.

If no error occurs to the $(n+2r)$-qubit cipher-text during transmission, the test qubits are always decoded as $|0\rangle^{\otimes r}|+\rangle^{\otimes r}$. However, if a nontrivial Pauli error occurs, the test qubits are decoded as $|0\rangle^{\otimes r}|+\rangle^{\otimes r}$ with probability no higher than 2^{-r}. To see this, decompose the Pauli error into its X and Z components, and without loss of generality, the X component is nontrivial. The overall effect of the extra CNOT can be found using the commutation relations in Section 3.2. An X_j during transmission becomes X_j and an extra X_{x_i} on the original cipher-text if $j \in S_{xi}$. Likewise, X_{z_j} becomes X_{z_j} with an extra X_{x_i} if $z_j \in T_{xi}$. An X_{x_i} decodes to itself. Thus x_i has an overall X error if an odd number of X occurs to $S_{xi} \cup T_{xi} \cup x_i$. As any nontrivial tensor product of X errors is equally likely to act on an even or odd number of qubits in a random subset, the probability for $x_1, \cdots, x_r$ to decode to $|0\rangle^{\otimes r}$ is 2^{-r}. A Z error is propagated to the z_i similarly. Note that the X and Z components act independently on the test qubits, and the x_i are unaffected by Z errors and the z_i are unaffected by X errors. This completes the proof that any nontrivial Pauli error is undetected with probability no more that 2^{-r}.

We now generalize the analysis for Pauli errors to the most general eavesdropping strategy. Using the framework of Section 3.1, let the received cipher-text be $\mathcal{E}(\rho) = \sum_{ij} e_{ij} P_i \rho P_j^\dagger$. Let P_0 be the identity Pauli error. Any nontrivial eavesdropping operation has $e_{00} < 1$.

Each set of random subsets corresponds to a detection scheme that distinguishes a set of Pauli errors $\mathcal{P}_I$ from its complement, and $P_0 \in \mathcal{P}_I$. The accepted output is $\mathcal{E}_a(\rho) \propto \sum_{P_i, P_j \in \mathcal{P}_I} e_{ij} P_i \rho P_j^\dagger$. Averaged over the random subsets, the unnormalized accepted state is given by

$$\mathcal{E}_a(\rho) = \sum_{ij} c_{ij} e_{ij} P_i \rho P_j^\dagger \tag{9}$$

where $c_{ij} \leq 2^{-r}$ except for $c_{00} = 1$. $\mathcal{E}_a(\rho)$ has high fidelity with respect to the original cipher-text.

For any eavesdropping strategy, the probability of Eve being undetected is at most $p_E = e_{00} + (1 - e_{00})2^{-r}$. We can relate e_{00} to the information gained by Eve. Without loss of generality, the cipher-text and Eve's ancilla are initially in a pure product state. After eavesdropping, the joint state remains pure. The classical information gained by Eve is bounded by the entropy of her reduced density matrix, which equals the entropy of $\mathcal{E}(\rho) = \sum_{ij} e_{ij} P_i \rho P_j^\dagger$ for a pure ρ. $\mathcal{E}(\rho)$ has an eigenvalue that is greater than e_{00}, hence the entropy is upper bounded by

$$H_2(e_{00}) + (1 - e_{00}) \log(2^{n+2r} - 1) = H_2(e_{00}) + \frac{1 - p_E}{1 - 2^{-r}} \log(2^{n+2r} - 1) \tag{10}$$

Eve's probability of eavesdropping without detection is roughly the same as the fraction of the classical information inaccessible to her.

5. The Quantum Vernam Cipher and Secret Sharing

We now explain the properties of the quantum Vernam cipher in terms of general connections [27] between secret communication and secret sharing [10,11]. A (classical or quantum)

secret sharing scheme divides a secret into *shares*. The secret is retrievable only with enough shares, which form the *authorized sets*. Other sets are *unauthorized*. In general, unauthorized sets can have partial information. We restrict to *perfect* schemes in which unauthorized sets have no information. A (k, n) *threshold* scheme is a perfect scheme in which any k out of n shares form an authorized set. In addition to the usual properties, quantum secret sharing schemes also obey the no-cloning theorem [28], so that complements of authorized sets are unauthorized. Finally, in pure state perfect quantum secret sharing schemes, complements of unauthorized sets are authorized.

Any private key encryption scheme (classical or quantum) which conveys a message from Alice to Bob but conceals it from Eve is a secret sharing scheme. The secret is divided into three shares: $\mathbf{A}$ and $\mathbf{B}$ are private shares for Alice and Bob, and $\mathbf{E}$ is the share communicated from Alice to Bob. Thus $\mathbf{A}$ and $\mathbf{B}$ represent the key, and $\mathbf{E}$ represents the cipher-text. By definition, $\{\mathbf{A}, \mathbf{E}\}$ and $\{\mathbf{B}, \mathbf{E}\}$ are authorized while $\mathbf{B}$ and $\mathbf{E}$ are unauthorized. In a quantum cipher, $\mathbf{A}$ is unauthorized. If additionally, the scheme is pure, $\{\mathbf{A}, \mathbf{B}\}$ is authorized: the scheme is a $(2, 3)$ threshold scheme.

The quantum Vernam cipher is an example of pure state threshold scheme described above. Entanglement is regenerated because $\mathbf{A}$ and $\mathbf{B}$ are identical shares. Errors on $\mathbf{E}$ are correctable because $\{\mathbf{A}, \mathbf{B}\}$ is authorized. Furthermore, in the quantum Vernam cipher: (*1*) Alice can encode an unknown message and her half of the key into the correctly distributed shares all by herself, and (*2*) errors on $\mathbf{E}$ are correctable using only local quantum operations and classical communication (LOCC) between Alice and Bob. We now characterize secret sharing schemes with these two properties. Property (*1*) holds for all pure state quantum secret sharing schemes in which the reduced density matrix of $\mathbf{B}$ is maximally mixed. This follows from the proof of the impossibility of quantum bit commitment [7], that two pure states with the same reduced density matrix in Bob's system can be transformed to each other by unitary operations acting outside Bob's system. Property (*2*) holds asymptotically if the entanglement between $\mathbf{A}$ and $\mathbf{B}$ (in ebits) in the secret sharing scheme is at least twice the size of $\mathbf{E}$ (in qubits). This follows from comparing the number of errors to be distinguished with the amount of information obtainable in the random hashing method [16].

As an example to construct a cipher from a secret sharing scheme with the above characterization, consider the (2,3) threshold scheme obtained from the 5-qubit 1-error correcting code [16,29], by assigning two qubits to each of $\mathbf{A}$ and $\mathbf{B}$, and one qubit to $\mathbf{E}$. The encoding circuit U_{enc} can be specified by how the *stabilizer* and the *encoded operations* evolve [30]. As U_{enc} is in the Clifford group [30], a circuit implementing U_{enc} can be constructed using a scheme in Ref. 30. The decoding circuit can be constructed similarly. The cipher obtained is shown in Fig. 4.

We find from Fig. 4 that the four possible Pauli errors in the cipher-text correlate with the EPR pairs being $|\Phi^+\rangle^{\otimes 2}$, $|\Phi^-\rangle^{\otimes 2}$, $|\Psi^+\rangle^{\otimes 2}$, and $|\Psi^-\rangle^{\otimes 2}$, where $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. The four cases are distinguishable by LOCC.

Cleve [31] derived another example of a cipher from a secret sharing scheme (Appendix C). It is a $(2, 3)$ threshold scheme in which all three shares are 3-dimensional.

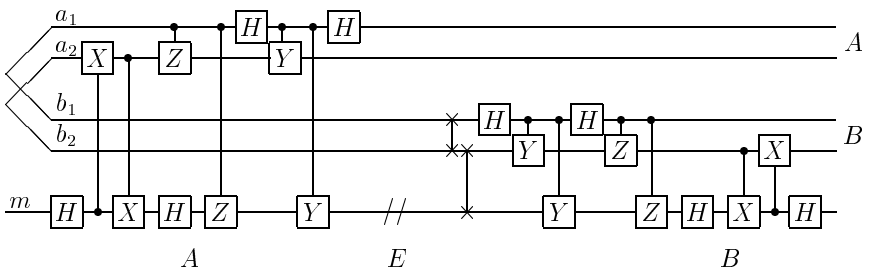


Fig. 4. The 5-bit code as a quantum cipher. In the circuit, $Y = iXZ$, $H = \frac{1}{\sqrt{2}}(X+Z)$, and a vertical line with $\times$ in both ends is a swap operation.

Errors on **E** cannot be corrected with LOCC, unless extra entanglement is available to Alice and Bob. On the other hand, this cipher requires less entanglement to conceal the message.

We can apply the connections between secret sharing and secret communication to the private quantum channel and teleportation [20] (see also Appendix D) which encrypts a quantum plain-text to a *classical* cipher-text using a quantum key.[j] In teleportation, *after* Alice's measurements, **E** is the outcome (k_1, k_2) to be communicated and **B** is the quantum state $Z^{k_2}X^{k_1}|\psi\rangle$ possessed by Bob. In the private quantum channel, $\mathbf{A} = \mathbf{B} = (k_1, k_2)$ is the classical key, and $\mathbf{E} = Z^{k_2}X^{k_1}|\psi\rangle$ is the communicated quantum state.[k] Viewing **A** and **B** in the second scheme as one share, both schemes are the same $(2, 2)$ threshold scheme with the quantum and classical shares interchanged. As a *mixed* state $(2, 2)$ scheme, errors on one share is not correctable, as we have seen in the private quantum channel. However, in teleportation, the classical share is broadcast and no correction is needed. Finally, the quantum Vernam cipher, with the three shares forming the state $\frac{1}{2}\sum_{k_1k_2}|k_1k_2\rangle\ |k_1k_2\rangle\ Z^{k_2}X^{k_1}|\psi\rangle$ is just the purification of the $(2, 2)$ scheme.

6. Conclusion

We have analyzed two important properties of the quantum Vernam cipher, the security of recycling keys and the reliability of the transmission, and have made comparisons with other related schemes. These results are summarized and extended to other existing schemes in the following table [34], which is explained next.

[j] Teleportation paradoxically communicates quantum states *securely* without quantum communication. The closely related remote state preparation [32,33] may not be secure.

[k] This provides an alternative proof for the lower bound of the classical key size, since an important classical share is at least twice the size of the quantum secret [11,27].

Type *CKM*	Example	Security of key recycling	Reliability
CCC	Classical one-time-pad	×	√
CCQ	Impossible		
CQC	Entanglement based key distribution [3]	×	
CQQ	Teleportation	×	√
QCC	Eavesdrop-detecting channel	√	×
QCQ	Private quantum channel	√	×
QQC	Superdense coding [21]	√*	×
QQQ	Quantum Vernam cipher	√	√
Q 0 C	BB84 [2]		
Q 0 Q	Establishing entanglement		

* Requires quantum back-communication.

In the table, the type of cryptographic protocol is specified by three elements: the communication channel (which is of the same type as the cipher-text C), the key K, and the message M to be conveyed. A 3-alphabet string represents these three elements *in order*. Q, C, and 0 respectively stand for the element being quantum, classical, and non-existing. The first property in question is the security of key recycling and the second property is reliability – whether the correct message is received with high probability. The security properties are based on Alice and Bob having an unjammable 2-way classical broadcast channel.

We can extrapolate the properties of the specific examples to classes of ciphers. For example, due to the use of an unjammable classical broadcast channel, all ciphers of the type C−− are reliable. In contrast, ciphers of the type Q−− are susceptible to errors, unless a large quantum key is available, such as in the quantum Vernam cipher. Since in the worst case the quantum channel is jammed, a general recovery procedure would involve LOCC and is effectively of the type CQQ (though the exact protocol needs not be teleportation). The very same unjammable classical channel in C−− cannot detect for eavesdropping, and used key can be compromised. The susceptibility in the quantum channel in Q−− is also the reason why it can detect eavesdropping and reject compromised keys. This quantum feature also allows key distribution to be possible.

The secure properties of the quantum Vernam cipher come at a price – it requires a quantum channel *and* pre-shared entanglement. In fact, for the same resources, one can use the quantum channel to establish entanglement and use the entanglement to teleport the state. The two methods are compared in Appendix E. We are not aware of a circumstance in which QQQ is more efficient than the hybrid method Q0Q + CQQ. This is not surprising in view of the above discussion, since the hybrid method exploits the advantages of both types of ciphers.

We have ensured security in key recycling by detecting errors in the cipher-text. This objective is very similar to that of message authentication – to reject a forged or altered

message with high probability. For example, our modification to the private quantum channel described in Section 4.2 can be viewed as an authentication step for the encrypted quantum message. For authentication, all U_i in Figure 3 can be omitted. The test qubits can detect both forging and tampering with high probability due to the random flip based on the $2r$-bit classical key. Forging succeeds with probability no better than 2^{-r} and the fidelity of an accepted message with respect to the origin cipher-text is of order $1 - \mathcal{O}(2^{-r})$. This means that authenticating n qubits given an insecure quantum channel and an authenticated 2-way classical channel requires only $2r$ bits of classical key and an extra $2r$ qubits of quantum communication. We can also drop the assumption of authenticity in the classical communication given a larger key to classically authenticate the classical messages, for example, using the Wegman-Carter method [35].[l] Recently, authentication protocols for quantum message using a classical key but no additional classical communication are proposed [12,13].

Returning to the connection with secret sharing, we have seen that in the quantum Vernam cipher, the quantum secret can be unlocked from an authorized set using only LOCC between the parties. Under the same conditions, hardly any information can be obtained in a recently proposed scheme [36] to share a classical secret. It will be interesting to understand the origin of such differences. It might be related to the amount of entanglement shared between the parties in the secret sharing scheme, and further investigation is underway. More generally, secret sharing schemes have mostly been analyzed assuming no or full cooperation between the different parties, and the security under LOCC remains an interesting area to be explored.

Acknowledgements

Stimulating discussions, mostly during the Workshop on Quantum Information and Computation held at the Aspen Center for Physics in June 2000, have contributed significantly to the results presented. The question on how to replace the classical key with a quantum one in the private quantum channel was initially raised by Julia Kempe and Xinlan Zhou. We attribute various connections between secret sharing and secret communication to interesting discussions with Hoi-Kwong Lo and Daniel Gottesman. We thank Hoi-Kwong Lo, Charlie Bennett, and Ike Chuang for helpful suggestions on recycling classical bits. We subsequently learned of ideas to recycle a classical key by Charlie Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner [15], and adapted their method in the present discussion. We also thank Charlie Bennett for enlightening discussions on the classification of cryptographic protocols. We learned of quantum message authentication from Howard Barnum and Alain Tapp after the initial submission of the manuscript. We greatly appreciate informative discussions with Richard Cleve on the cipher in Appendix C, Michael Nielsen on Shannon's classical results, John Preskill on the malleability of the ciphers, and John Smolin on random hashing. We thank Hoi Fung Chau, David DiVincenzo, and Michelle Mosca for enjoyable discussions, and Charlie Bennett, Hoi Fung Chau, David

[l] We need to authenticate a 1-bit message from Bob and a $(2nr + r^2)$-bit message from Alice, requiring two keys with $4(r + \log\log(2nr + r^2)) \times \log(2nr + r^2)$ and $4(r + \log\log(2r + r^2)) \times \log(2r + r^2)$ bits.

DiVincenzo, Hoi-Kwong Lo, and Barbara Terhal for critical comments on the manuscript. We acknowledge support from the National Security Agency and the Advanced Research and Development Activity through the Army Research Office contract number DAAG55-98-C-0041.

References

1. P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", In Proc. 35^{th} Annual Symposium on Foundations of Computer Science, p. 124 (1994), IEEE Computer Society Press, Los Alamitos, CA.
2. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proc. of IEEE International Conference on Computers, Systems and Signal Processing", p. 175-179, IEEE Press, New York, December 1984.
3. A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem", Phys. Rev. Lett., **67** (1991) p. 661-63.
4. D. Mayers, "Quantum Key Distribution and string oblivious transfer in noisy channels", In Advances in Cryptology – Proceedings of Crypto '96, (Springer-Verlag, New York, 1996) p. 343-57.
5. H.-K. Lo and H. F. Chau, "Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances", Science, **283** (1999) p. 2050-56. See also arXive e-print quant-ph/9803006.
6. D. Mayers, "Unconditionally Secure Quantum Bit Commitment is Impossible", Phys. Rev. Lett., **78** (1997) p. 3414-17.
7. H.-K. Lo and H. F. Chau, "Is Quantum Bit Commitment Really Possible?", Phys. Rev. Lett., **78** (1997) p. 3410-13. See also arXive e-print quant-ph/9603004.
8. A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channels", In Proc. 41^{st} Annual Symposium on Foundations of Computer Science, p. 547 (2000), IEEE Computer Society Press, Los Alamitos, CA. See also arXive e-print quant-ph/0003101.
9. P. O. Boykin and V. Roychowdhury, "Optimal Encryption of Quantum Bits", arXive e-print quant-ph/0003059.
10. R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret", Phys. Rev. A, **82** (1999) p. 648-51. See also arXive e-print quant-ph/9901025.
11. D. Gottesman, "On the theory of quantum secret sharing", arXive e-print quant-ph/9910067.
12. H. Barnum, "Quantum message authentication codes", arXive e-print quant-ph/0103123.
13. C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, personal communication.
14. G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", J. American Inst. Elec. Eng., **55** (1926) p. 109-15.
15. C. H. Bennett, G. Brassard, and S. Breidbart, "How to re-use a one time pad safely even if P=NP", (1982) unpublished. C. H. Bennett, G. Brassard, S. Briedbart, and S. J. Wiesner, "Eavesdropping-detecting quantum communications channel", IBM Technical Disclosure Bulletin **26**, (1984) p. 4363-4366. The eavesdrop-detecting channel as reviewed in the paper is simplified, omitting the error correction procedure and replacing the check sums by random subset parities.
16. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed State Entanglement and Quantum Error Correction", Phys. Rev. A, **54** (1996) p. 3824-51. See also arXive e-print quant-ph/9604024.
17. Y.-S. Zhang, C.-F. Li, and G.-C. Guo, "Quantum key distribution via quantum encryption", arXive e-print quant-ph/0011034.
18. The quantum Vernam cipher randomizes the quantum plain-text in two conjugate bases. The

scheme in Ref. 17 randomizes the quantum plain-text in one basis, and does not conceal it completely.
19. C. E. Shannon, "Communication theory of secrecy systems", Bell Systems Technical Journal, **28** (1949) p. 656-715.
20. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels", Phys. Rev. Lett., **70** (1993) p. 1895-98.
21. C. H. Bennett and S. J. Wiesner, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States", Phys. Rev. Lett, **69** (1992) p. 2881-2884.
22. C. H. Bennett and G. Brassard and C. Crépeau and U. M. Maurer, "Generalized Privacy Amplification", IEEE Trans. on Information Theory, **41** (1995) p. 1915-23.
23. I. L. Chuang and M. A. Nielsen, "Prescription for experimental determination of the dynamics of a quantum black box", J. Mod. Opt, **44** (1997) p. 2455-67. See also arXive e-print quant-ph/9610001.
24. E. Knill and R. Laflamme, "Concatenated Quantum Codes", LANL Report LAUR-96-2808 (1996), See also arXive e-print quant-ph/9608012.
25. See for example, S. Goldwasser and M. Bellare, *Lecture notes on Cryptography* (1997) p. 59-61, Available at http://www-cse.ucsd.edu/users/mihir/.
26. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, New York, 1991.
27. H.-K. Lo and D. Gottesman, personal communication.
28. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", Nature, **299** (1982) p. 802-803.
29. R. Laflamme, C. Miquel, J. Paz, and W. H. Zurek, "Perfect Quantum Error Correction Code", Phys. Rev. Lett., **77** (1996) p. 198. See also arXive e-print quant-ph/9602019.
30. D. Gottesman, "Stabilizer Codes and Quantum Error Correction", PhD thesis, California Institute of Technology, Pasadena, CA, 1997. See also arXive e-print quant-ph/9705052.
31. R. Cleve, personal communication.
32. H.-K. Lo, "Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity", Phys. Rev. A, **62** (2000) p.012313. See also arXive e-print quant-ph/9912009.
33. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, B. M. Terhal, and W. K. Wootters, "Remote State Preparation", arXive e-print quant-ph/0006044.
34. C. H. Bennett, personal communication.
35. M. N. Wegman and J. L. Carter, "New Hash Functions and Their Use in Authentication and Set Equality", J. of Computer Science and System Sciences, **22** (1981) p. 265-79.
36. B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, "Hiding bits in Bell states", arXive e-print quant-ph/0011042.

Appendix A. Definitions of some Ciphers

We briefly describe the ciphers which are not reviewed elsewhere in this paper:

- *Entanglement based key distribution* Alice and Bob share a large number of $|\Phi^+\rangle$. They measure their halves of the EPR pairs independently in the $\{|0\rangle, |1\rangle\}$ basis. Their measurement results can be used as keys. If Alice and Bob are given a quantum channel instead, they first establish pure entanglement with the standard test procedures.
- *BB84* Alice sends to Bob $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ chosen at random, and Bob measures

them in random basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. They subsequently announce their bases. Only the measurement results obtained in the matching basis are used. A sufficient number of the results are announced and compared to test for eavesdropping. Upon passing the test, privacy amplification [22] is applied to the results not announced to establish classical keys.

- *Superdense coding* Alice and Bob share one copy of $|\Phi^+\rangle$. Alice can send 2 classical bits c_1, c_2 securely to Bob as follows. Alice applies $X^{c_1}Z^{c_2}$ on her half of $|\Phi^+\rangle$ and sends it to Bob. Bob can determine c_1, c_2 by a Bell measurement on both qubits.

Appendix B. Recovery of Message without the Cipher-text

Without loss of generality, let the message be $|\psi\rangle = a|0\rangle + b|1\rangle$. Ordering the registers as (a_1, b_1, a_2, b_2, m), the system has initial state $|\Phi^+\rangle|\Phi^+\rangle|\psi\rangle$. The state changes:

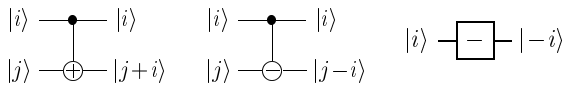
$$
\begin{aligned}
& \frac{1}{2}\left[\ |0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\ \right](a|0\rangle + b|1\rangle) \\
\rightarrow\ & \frac{1}{2}\left[\ |0000\rangle(a|0\rangle + b|1\rangle) + |0011\rangle(a|0\rangle - b|1\rangle)\right. \\
& \left. + |1100\rangle(a|1\rangle + b|0\rangle) + |1111\rangle(-a|1\rangle + b|0\rangle)\ \right] \qquad \text{(B.1)} \\
\rightarrow\ & \frac{1}{2}\left[\ a(|0000\rangle + |0011\rangle) + b(|1100\rangle + |1111\rangle)\ \right] \\
\oplus\ & \frac{1}{2}\left[\ b(|0000\rangle - |0011\rangle) + a(|1100\rangle - |1111\rangle)\ \right] \qquad \text{(B.2)} \\
\rightarrow\ & \frac{1}{2}\left[\ a(|0000\rangle + |0011\rangle)|0\rangle + b(|1100\rangle + |1111\rangle)|1\rangle\ \right] \\
\oplus\ & \frac{1}{2}\left[\ b(|0000\rangle - |0011\rangle)|0\rangle + a(|1100\rangle - |1111\rangle)|1\rangle\ \right] \qquad \text{(B.3)} \\
=\ & \frac{1}{4}\left[\ (|00\rangle + |11\rangle)(|00\rangle + |11\rangle)(a|0\rangle + b|1\rangle)\right. \\
& \left. + (|00\rangle - |11\rangle)(|00\rangle + |11\rangle)(a|0\rangle - b|1\rangle)\ \right] \\
\oplus\ & \frac{1}{4}\left[\ (|00\rangle + |11\rangle)(|00\rangle - |11\rangle)(b|0\rangle + a|1\rangle)\right. \\
& \left. + (|00\rangle - |11\rangle)(|00\rangle - |11\rangle)(b|0\rangle - a|1\rangle)\ \right] \qquad \text{(B.4)}
\end{aligned}
$$

describe the encoding (Eq. (B.1)), the removal of m (Eq. (B.2)), and the decoding by Bob after he substitutes $|0\rangle$ for m (Eq. (B.3)). The $\oplus$ denotes a mixture of states. The decoded state is rewritten in Eq. (B.4), to which the syndrome measurement described in Section 3.2 is applicable.

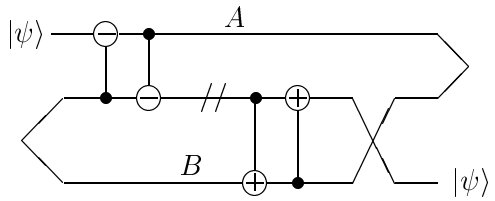
Appendix C. Quantum Secret Sharing Scheme as Secure Quantum Channel

We describe another cipher due to Cleve [31] constructed from a $(2, 3)$ threshold quantum secret sharing scheme. The plain-text $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$ is a three dimensional state

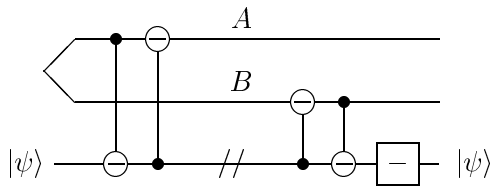
(a qutrit). We define the following gates acting on qutrits:



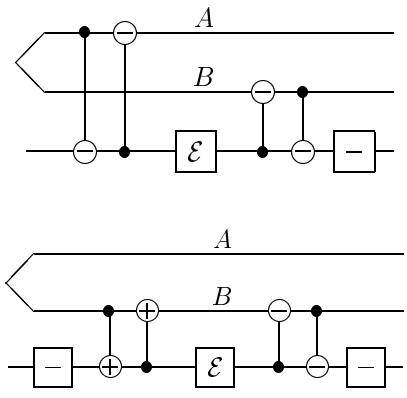
where sums and differences are taken modulo 3. The proposed scheme can be represented by the following circuit:



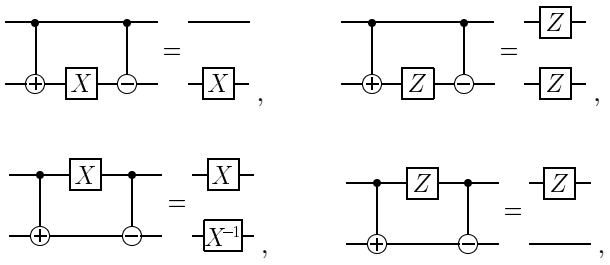
in which the maximally entangled state is $\frac{1}{\sqrt{3}}(|00\rangle + |12\rangle + |21\rangle)$, A, B represent the private shares of Alice and Bob, and // represents a transmission from Alice to Bob. The regenerated entangled state is explicitly marked. Encoding is performed locally by Alice. As a $(2, 3)$ threshold scheme, any error in the transmitted qutrit is correctable. However, correction *cannot* be performed using only LOCC operations by Alice and Bob. To see this, we first rearrange the qutrits in the circuit and redefine the maximally entangled state as $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$.



We can now easily find the effect of an error $\mathcal{E}$ during transmission, for the following circuits are equivalent:



We consider an error basis on a qutrit generated by X and Z where $X|j\rangle = |j+1\rangle$ and $Z|j\rangle = e^{2\pi ij/3}|j\rangle$. Using the commutation relations

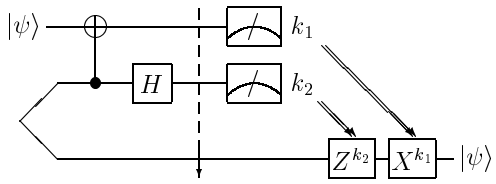


the overall effects due to the errors X^t and Z^t can be obtained:

The 9 possible errors are correlated with 9 orthogonal maximally entangled states, which are globally distinguishable but indistinguishable with LOCC, or else Alice and Bob can identify maximally entangled states from the maximally mixed state and distill entanglement out of nothing.

Appendix D. Teleportation

Without loss of generality, consider the teleportation of a pure state $|\psi\rangle = a|0\rangle + b|1\rangle$ using the following circuit:



It is easily verified that the initial state $\frac{1}{\sqrt{2}}(a|0\rangle + b|1\rangle)(|00\rangle + |11\rangle)$ is transformed to

$$\frac{1}{2}\left[\ |00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|0\rangle - b|1\rangle)\right. \tag{D.1}$$

$$\left. + |10\rangle(a|1\rangle + b|0\rangle) + |11\rangle(-a|1\rangle + b|0\rangle)\ \right] \tag{D.2}$$

$$= \frac{1}{2}\sum_{k_1 k_2} |k_1\rangle|k_2\rangle Z^{k_2} X^{k_1}|\psi\rangle \tag{D.3}$$

right before measurement. The measurement results k_1, k_2 are sent over a classical channel to recover $|\psi\rangle$.

Appendix E. Comparison of Resources

We compare the asymptotic resources required to send n qubits securely by (1) the quantum Vernam cipher (QQQ) and (2) establishing entanglement and teleporting (Q0Q + CQQ). We compare the net amount of entanglement consumed, allowing both schemes n uses of an insecure quantum channel and unlimited uses of a 2-way classical broadcast channel. The quantum Vernam cipher uses $2n(1-F)$ ebits where F is the recyclable fraction of entanglement. Teleportation uses $n(1-D_2)$ ebits where nD_2 ebits are distillable from n uses of the quantum channel. Hence, teleportation is more efficient if and only if $F \leq (1+D_2)/2$.

In the following comparisons, we use more optimal recycling strategies than that in Section 4.1. Without eavesdropping, $F \approx D_2 \approx 1$. If Eve measures every qubit in the computation basis, Z occurs randomly. Hence $D_2 = 0$ and $F = 1/2$ since the EPR pairs detecting X errors are intact. If I, X, Z, XZ occur with probabilities 1/2, 1/6, 1/6, 1/6, $D_2 = 0$ and $F = 0.1037$. For a completely random Pauli channel, $D_2 = F = 0$. Hence for the first two cases, the two methods are equally efficient. For the last two cases, teleportation is much more efficient.